NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Regional

National

International

Banking and Finance Industry

Chemical and Hazardous Materials Sector

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

Government Sector (including Schools and Universities)

Information Technology and Telecommunications

National Monuments and Icons

Postal and Shipping

Public Health

Transportation

Water and Dams

North Dakota Homeland Security Contacts

North Dakota

Officials to test Minot proppant after oilfield waste found radioactive. The North Dakota Department of Health said January 23 it will be testing bags filled with proppant sand stacked in Minot for radioactivity. The decision stems from recent news the Williston landfill rejected 23 loads of oilfield waste since June due to radioactive contamination. An independent testing firm called in to investigate the situation found ceramic proppant, as well as filter socks used in the process of preparing “frack sand” to be pumped into the ground, to be radioactive. The materials found were determined to be naturally occurring radioactive materials, but the quantities of the materials turning up in testing is far above the levels found in nature. Those materials were traced to proppant originating in China, according to the director of the North Dakota Department of Health’s Air Quality Division. Source: http://www.minotdailynews.com/page/content.detail/id/562393/Officials-to-test-Minot-proppant-after-oilfield-waste-found-radioactive.html?nav=5010

Corps to increase water releases at Garrison Dam, now that Bismarck area has stable ice cover. The U.S. Army Corps of Engineers plans to gradually increase water releases from Garrison Dam on the Missouri River in North Dakota over the next several weeks, the Associated Press reported January 20. The Corps said a stable ice cover has been established on the river at Bismarck, allowing officials to release more water through the dam upstream without leading to river rises near the capital city. The Corps said the river level at Bismarck typically rises during the freeze-over period. That happened earlier this month, and higher-than-normal river stages in some areas prompted the National Weather Service to issue a flood warning. The river stayed below flood stage, there was no damage, and the warning has since been canceled. Source: http://www.therepublic.com/view/story/93d9ed8e061d4f2eb870f8caf01268a8/ND--Garrison-Dam-Releases/

Feds investigating ND water tower shooting. Officials in Bismarck, North Dakota, said a water tower on Fort Berthold Indian Reservation has been shot full of holes. The federal Bureau of Reclamation said the 750,000-gallon water tower near Parshall was shot early this month. The agency said a reward is being offered for tips. Source: http://www.jamestownsun.com/event/article/id/152954/group/homepage/

Regional

(Minnesota) **Bloomington duo accused of mortgage fraud.** Two Bloomington residents were arraigned January 26 in Minneapolis on charges they ran an $8 million equity-stripping scheme under the guise of a nonprofit that claimed to help troubled homeowners avoid foreclosure. The residents were each charged January 19 in a sealed indictment with conspiracy, fraud, and money laundering involving transactions that took place from 2005 through October 2007. One of the defendants owned and operated Unified Home Solutions (UHS) and American Mortgage Lenders (AML), a mortgage brokerage that facilitated the transactions, the indictment says. It notes the UHS owner told homeowners facing foreclosure that he offered a rescue program backed by investors who would buy their homes and sell them back after they had regained their financial footing. The indictment says the mortgages were obtained with fraudulent financial information. Investors collected a “risk fee,” generally 3 percent of the purchase price, but most of the equity in the home went to UHS and AML, according to an affidavit filed in the case by an Internal Revenue Service (IRS) criminal investigator. She said UHS, AML, and their owner facilitated the sale of about 79 properties; fewer than five avoided foreclosure. Source: http://www.startribune.com/business/138169374.html

(Minnesota) **Federal gang investigation locks down all Minn. prisons.** The prison system in Minnesota was put on lockdown January 24, while federal agents worked to break up a major gang. Investigators told KMSP 9 Eden Prairie they hope the inmate restrictions will stop any prisoners from alerting suspects on the streets that they are being sought. Investigators are currently seeking at least two people wanted on murder charges while 9,000 inmates are seeing their movements restricted, meaning they can no longer see visitors or make phone calls. Agents are serving warrants both inside and outside prison walls in a search for at least seven people on charges ranging from murder to racketeering. Source: http://www.myfoxtwincities.com/dpp/news/minnesota/federal-gang-investigation-locks-down-all-minn-prisons-jan-24-2012#ixzz1kUICHJnd

National

Nothing Significant to Report

International

Powder mailings sent to Israeli embassies. Israeli embassies and consulates at six U.S. and European locations received mailings marked “anthrax” that carried a nontoxic white powder, Agence France-Presse (AFP) reported January 24. The envelopes arrived at Israeli embassies in London, England, The Hague, Netherlands, and Brussels, Belgium, AFP quoted Israeli news reports as saying. Consulates in New York, Houston, and Boston received similar mailings. Source: http://www.nti.org/gsn/article/suspicious-powder-sent-israeli-foreign-delegations/

Banking and Finance Industry

Treasury designates major Iranian state-owned bank. The U.S. Department of the Treasury January 23 designated Iran’s third-largest bank, Bank Tejarat, for providing financial services to several Iranian banks and firms already subject to international sanctions for involvement in Iran’s weapons of mass destruction (WMD) proliferation activities. With the January 23 action, 23 Iranian-linked financial institutions, including all of Iran’s largest state-owned banks, have been sanctioned by the United States based on their involvement in Iran’s illicit activities. Bank Tejarat was designated pursuant to Executive Order (E.O.) 13382 (Blocking Property of WMD Proliferators and Their Supporters) for providing financial services to Bank Mellat, the Export Development Bank of Iran (EDBI), the Islamic Republic of Iran Shipping Lines (IRISL), and the Ministry of Defense for Armed Forces Logistics (MODAFL), all of which were previously designated by Treasury or the Department of State for involvement in Iran's WMD proliferation activities. Trade Capital Bank also was designated January 23 for providing financial services to EDBI, and for being owned or controlled by Bank Tejarat. Bank Tejarat has nearly 2,000 branches throughout Iran, as well as foreign branches in France and Tajikistan. Trade Capital Bank is a Belarus-based bank owned by Bank Tejarat. Bank Tejarat has directly facilitated Iran's illicit nuclear efforts. For example, in 2011, Bank Tejarat facilitated the movement of tens-of-millions of dollars in an effort to assist the Atomic Energy Organization of Iran's ongoing effort to acquire uranium. Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1397.aspx

Fraud alert involving e-mail intrusions to facilitate wire transfers overseas. The FBI observed a trend in which cyber criminals are compromising the e-mail accounts of U.S. individuals and businesses and using variations of the legitimate e-mail addresses associated with the victim accounts to request and authorize overseas transactions, according to a January 20 alert. The wire transfers are being sent to bank accounts of individuals typically located domestically or in Australia, and the funds are being sent directly to Malaysia. Investigations found some of the money mules in the United States and Australia are victims of a romance scam and are asked to further transfer the funds to Malaysia. As of December 2011, the attempted fraud amounts were about $23 million; with actual victim losses about $6 million. This type of fraud has affected banks, broker/dealers, credit unions, and other institutions. In a typical scenario, the cyber criminal will send an e-mail to a financial institution, brokerage firm employee, or the victim's financial adviser pretending to be the victim and request the balance of the victim's account. When the request is successful, the cyber criminal then sends another e-mail providing a reason why they can only communicate via e-mail and asks that a wire transfer be initiated on their behalf. The excuse is typically based on an illness or death in the family that prevents the account holder from conducting business as usual. Source: http://www.ic3.gov/media/2012/EmailFraudWireTransferAlert.pdf

New ZeuS variant 'Citadel' comes with customer support. During his expeditions in the hacking underground, a security researcher came across a new variant of the bank-account-stealing ZeuS Trojan called Citadel. Citadel's developers mainly address customers not satisfied with the support offered by other malware providers. The fact that malware developers rarely make sure bugs in their products are patched up is seen as a business opportunity for Citadel's owners. This is why they offer a bug reporting and suggestions mechanism via a ticketing system, allowing customers to file as many complaints as they want without having to contact the developer on instant messaging channels. Clients can also submit their own applications in what appears to be a social network. For $2,400 plus a monthly fee, cybercriminals can purchase a Citadel package comprised of a bot builder and a botnet administration panel. Among other features and add-ons that the trojan's creators offer, there is one that detects if the victim's keyboard is Russian or Ukrainian. It is known that hackers fear Russian authorities more than anything else because they are known to track down and prosecute those who commit crimes in the virtual environment. This is why this particular variant of ZeuS shuts itself down as soon as it detects the aforementioned keyboards. Source:

http://news.softpedia.com/news/New-ZeuS-Variant-Citadel-Comes-with-Customer-Support-248032.shtml

Chemical and Hazardous Materials Sector

(Tennessee) **Regulators say flood barriers may not protect TVA's nuclear plants.** Sand baskets that the Tennessee Valley Authority installed at dams in Tennessee to protect its nuclear plants from a worst-case flood could fail, according to a Nuclear Regulatory Commission (NRC) letter dated January 25. The NRC said the baskets are not capable of standing up to the impact of debris barreling down the Tennessee River in a massive flood. "There is potential for this debris to damage the baskets or push the individual baskets apart, causing a breach," the letter said. "There would be no time to repair the baskets because the flood would already be in progress." The sand-filled, wire mesh baskets were placed around Cherokee, Fort Loudon, Tellico, and Watts Bar dams and earthen embankments. The electric power producer had told the NRC in 2010 that a project to resolve flooding concerns would extend into 2016 with dam modifications handled by the U.S. Army Corps of Engineers. Lack of federal funds is expected to cause more delay. The NRC said the baskets are acceptable as a temporary fix. Source: http://www.tennessean.com/article/20120126/NEWS11/301260077/Regulators-say-flood-barriers-may-not-protect-TVA-s-nuclear-plants?odyssey=nav|head

Commercial Facilities

IP D-Day: Major providers, vendors to go IPv6 June 6. It has been in the works for more than a decade, but the next-generation IPv6 protocol will officially go live in some major corners of the Internet in 2012, Dark Reading reported January 24. The Internet Society has deemed June 6 as World IPv6 Day, when Google, AT&T, Facebook, Comcast, Cisco, and others plan to flip the switch to the new IP protocol. IPv6 has been available in most products for some time, and various organizations and government agencies have test-run the protocol. Other nations, such as Japan and France, have already broadly rolled out IPv6. Meanwhile, IPv4 has outlasted some predictions it would have run out of address space by now, and IPv6 has exponentially more address space that can better accommodate the explosion of IP devices. Like any new technology rollout, security experts say the transition to IPv6 could introduce new bugs into the ecosystem. Among the companies participating in the IPv6 cutover June 6 are Google, Facebook, Microsoft Bing, Yahoo!, AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, XS4All, Cisco, and D-Link. The ISPs going to IPv6 — AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, and XS4ALL — will roll out the new protocol in their networks so that at least 1 percent of their wireline residential subscribers who visit other IPv6-enabled Web sites will get there via IPv6. They plan to make IPv6 a big part of their services, while new home routers from Cisco and D-Link will enable IPv6 by default. Source: http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232500387/

Communications Sector

Hacktivists turn to DNS hijacking. Hacktivists have added a new tactic to their arsenal: redirecting all traffic from a target company's Web site, Dark Reading reported January 26. According to a blog written by a security expert from Internet Identity (IID), politically motivated attackers are now using DNS hijacks, which redirect all traffic from a victim's legitimate Web site (and often all the e-mail and back-end transactions, too) to a destination of the attacker's choosing. "A determined criminal can set up a fake look-alike destination site to dupe customers into revealing credentials or downloading malware," the expert stated. Many companies pay little, if any, attention to securing their domain registrations, and most do not continuously monitor their DNSes to make sure they're resolving properly around the world, making them vulnerable to attack, the blog said. "The first indication most victims have of a DNS hijack is that their website traffic slows to a trickle," it noted. "Then they have to figure out why, and DNS is rarely the first thing they think of, which lengthens the time to mitigate the attack." On January 22, the domain name UFC.com was hijacked by a hacktivist group, IID reported. On January 23, that same group, called UGNazi, hijacked two domain names, coach.com and coachfactory.com, belonging to luxury goods maker Coach Inc. Both Coach and UFC registered their domains at Network Solutions, IID reports. "The criminals hijacked the domains by accessing the companies' domain management accounts at Network Solutions," the blog stated. "It's currently unclear how they did so. In such cases, the cause is usually weak or compromised user passwords, or a website vulnerability at the registrar." Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232500513/hacktivists-turn-to-dns-hijacking.html

IP D-Day: Major providers, vendors to go IPv6 June 6. It has been in the works for more than a decade, but the next-generation IPv6 protocol will officially go live in some major corners of the Internet in 2012, Dark Reading reported January 24. The Internet Society has deemed June 6 as World IPv6 Day, when Google, AT&T, Facebook, Comcast, Cisco, and others plan to flip the switch to the new IP protocol. IPv6 has been available in most products for some time, and various organizations and government agencies have test-run the protocol. Other nations, such as Japan and France, have already broadly rolled out IPv6. Meanwhile, IPv4 has outlasted some predictions it would have run out of address space by now, and IPv6 has exponentially more address space that can better accommodate the explosion of IP devices. Like any new technology rollout, security experts say the transition to IPv6 could introduce new bugs into the ecosystem. Among the companies participating in the IPv6 cutover June 6 are Google, Facebook, Microsoft Bing, Yahoo!, AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, XS4All, Cisco, and D-Link. The ISPs going to IPv6 — AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, and XS4ALL — will roll out the new protocol in their networks so that at least 1 percent of their wireline residential subscribers who visit other IPv6-enabled Web sites will get there via IPv6. They plan to make IPv6 a big part of their services, while new home routers from Cisco and D-Link will enable IPv6 by default. Source: http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232500387/

Solar flare may hit satellite communications, GPS. A burst of radiation on the sun's surface may trigger a geomagnetic storm on Earth January 24 that could disrupt satellite communications and the Global Positioning System by mid-morning, scientists at the Space Weather Prediction Center said January 23. The eruption — called a solar flare — has also sent billions of tons of matter streaming toward Earth from the sun's surface at millions of miles per hour in what scientists call a coronal mass ejection, according to a physicist at the center in Boulder, Colorado. The radiation storm could create unusually intense flares of the aurora borealis — the northern lights — and has caused some international airlines to divert planes from polar routes to courses where radio communication is less likely to be affected, the physicist said. A new National Aeronautics and Space Administration satellite called the Solar Dynamics Observatory is vastly improving the ability of scientists to predict the violent magnetic storms that threaten Earth and to understand the mysterious nature of solar physics, the physicist said. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/24/MNJJ1MTCTM.DTL

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(Oregon) **Emergency alert test reaches less than one percent.** A test of the Portland, Oregon area's emergency alert system failed January 26. At 11 a.m. city and county officials tried to reach more than 300,000 communication devices in a "stress test" of emergency capabilities. Officials said the test signal reached less than 1 percent of devices — only about 2,100. The director of the Portland Bureau of Emergency Management said tests have been successful when a single neighborhood was contacted, with just a few hundred devices. She said in the event of actual emergencies, getting out customized local messages may prove more important. Having the system work citywide is important enough that officials are planning another test, as soon as the week of January 30. The city's vendor, First Call, said Portland has a customized system and it is looking into why it performed so poorly January 26. Source: http://news.opb.org//article/emergency-alert-test-reaches-less-one-percent/

(Kentucky) **Sheriff's office says deputy's cars targeted by thieves.** The Jefferson County Sheriff's Department in Kentucky was the target of criminals twice recently, WLKY 32 Louisville reported January 25. In one case, the sheriff's office said a rifle was stolen after the door of a marked vehicle at an off-duty deputy's Hikes Point home was pried open. The internal affairs unit is investigating whether any procedure or policy was violated. In the other incident, a stun gun was also stolen from another marked sheriff's vehicle after the vehicle's window was broken out. It was parked at an off-duty deputy's home in west Louisville. Source: http://www.wlky.com/r/30292735/detail.html

Police use of GPS is ruled unconstitutional by court. On January 23, the Supreme Court unanimously ruled police violated the Constitution when they placed a Global Positioning System tracking device on a suspect's car and monitored its movements for 28 days. A set of overlapping opinions in the case collectively suggested a majority of the justices are prepared to apply broad privacy principles to bring the Fourth Amendment's ban on unreasonable searches into the digital age, when law enforcement officials can gather extensive information without ever entering an individual's home or vehicle. An overlapping array of justices were divided on the rationale for the decision, with the majority saying the problem was the placement of the device on private property. Five justices also discussed their discomfort with the government's use of or access to various modern technologies, including video surveillance in public places, automatic toll collection systems on highways, devices that allow motorists to signal for roadside assistance, location data from cell phone towers, and records kept by online merchants. Source: http://www.nytimes.com/2012/01/24/us/police-use-of-gps-is-ruled-unconstitutional.html?_r=1&ref=us

(Utah) **Utah Chiefs of Police Website hacked by Anonymous group.** A hacker group protesting Congress' controversial anti-piracy bills was able to shut down several Web sites January 18, including the site for the Utah Chiefs of Police Association. A group calling itself Anonymous is believed to have hacked into several Web sites including the U.S Justice Department, Universal Music, the Motion Picture Industry of America, and other recording sites. Also included in the list of Web sites taken down was www.utahchiefs.org. The Web site had a message January 20 that said, "Our website is temporarily closed for maintenance." The executive director of the association said his group's site was not even fully developed yet. Names, addresses, and phone numbers of many Utah police chiefs were on the Web site, but most of that information is already public. Source: http://www.deseretnews.com/article/705397751/Utah-Chiefs-of-Police-website-hacked-by-ANONYMOUS-group.html

Energy

(California) **3 arrested in Moorpark copper theft.** Three men were arrested January 22 on suspicion of stealing thousands of dollars worth of copper wire from a Southern California Edison facility in Moorpark, California, authorities said. The suspects were arrested following a theft of copper and tools at least six times in recent months from the Edison plant near Gabbert Road and Highway 118. Edison officials estimate their total loss to be over $100,000 from the recent burglaries. Moorpark police detectives were conducting surveillance at the Edison plant about 3:30 a.m. January 22 when they saw three people cut through a fence and enter the property. About 90 minutes later, the suspects left in a vehicle with stolen wire from the plant, officials said. Authorities stopped the vehicle and found about $25,000 worth of copper wire inside. Source: http://www.vcstar.com/news/2012/jan/22/3-arrested-in-moorpark-copper-theft/

Food and Agriculture

(Maine) **FDA orders smoked salmon held after Listeria detected.** Using its newly expanded authority under the Food Safety Modernization Act, the U.S. Food and Drug Administration (FDA) ordered the detention of cold-smoked salmon in Maine after inspectors found Listeria monocytogenes in equipment and in areas throughout a food-processing and storage facility, Food Safety News reported January 25. The company, Mill Stream Corp. of Hancock, then agreed to destroy its cold-smoked salmon under FDA supervision, the federal agency said in a news release January 24. The FDA said Listeria was detected at the processing plant during an inspection in December. The agency news release explained that the FDA may order the detention of food when an investigator has a reason to believe it is adulterated or misbranded. Food subject to such a detention order may not be moved, without agency permission, until the agency releases it or the detention order expires. A detention order may remain in place for up to 30 days. Source: http://www.foodsafetynews.com/2012/01/fda-orders-smoked-salmon-held-after-listeria-detected/

Jones' Seasoning recalls products over possible Salmonella contamination. Jones' Seasoning Blends LLC is voluntarily recalling its products — Jones' Mock Salt Original and Jones' Mock Salt Spicy Southwest Blend on possible contamination of Salmonella, RTTNews reported January 24. Jones' Mock Salt Original and Jones' Mock Salt Spicy Southwest Blend are seasoning products containing organic garlic, organic onion, organic celery seeds, organic black pepper, and organic orange peel as some of the ingredients. Salmonella contamination of the celery seeds ingredient used in Jones Mock Salt is the cause for the recall of the products. Jones Seasoning Blends LLC said that it is not responsible for the Salmonella contamination, and that the supplier of the celery seeds has been recalling the product. The affected products were directly distributed to grocery stores and markets in California, Minnesota, and Washington as well as sold through Internet orders. Source: http://www.rttnews.com/Story.aspx?type=bs&Id=1803506&Category=FDARecall

Rancid baby cereal recalled in Canada. One illness was reported, and the Canadian Food Inspection Agency (CFIA) and Loblaw Companies Ltd. are warning the public not to consume President's Choice Organics infant cereals because the products may have an unpleasant rancid odor, or taste, Food Safety News reported January 21. The cereal importer, Loblaw Companies Ltd. of Toronto, Ontario, is recalling all lot codes of eight types of President's Choice Organics infant cereal. The affected products have been distributed nationally in Canada. In its recall alert, the CFIA said the cereal should not be consumed if has an unusual odor or smells "off." Infants fed any of the recalled cereal should not be fed any more of it, and should be monitored for symptoms such as vomiting and diarrhea. Source: http://www.foodsafetynews.com/2012/01/rancid-baby-cereal-recalled-in-canada/

Government Sector (including Schools and Universities)

(Utah) **Utah teens arrested in alleged school bombing plot.** Two Roy, Utah high school students plotted to set off explosives during a school assembly and steal a plane to make their getaway, police said January 26. The students prepared by logging hundreds of hours on flight simulator software on their home computers, and they planned to take a plane at Ogden Hinckley Airport, the Roy police spokeswoman said. The two students were pulled out of school January 25 after authorities learned of the plot. They were held for hours of questioning and arrested. An after-school bomb sweep found no explosives at Roy High School, about 30 miles north of Salt Lake City. One of the students was held on $10,000 bail at Weber County jail on suspicion of conspiracy to commit mass destruction. The other student, a juvenile, was in custody at Weber Valley Detention Center on the same charge. Prosecutors are weighing possible additional charges. Both students had "absolute knowledge of the security systems and the layout of the school," the Roy police spokeswoman said. "They knew where the security cameras were. Their original plan was to set off explosives during an assembly. We don't know what date they were planning to do this, but they had been planning it for months." Source: http://www.foxnews.com/us/2012/01/27/utah-teens-arrested-in-alleged-school-bombing-plot/?intcmp=trending

FTC site still down after Anonymous hack; anti-piracy fallout spreads. The Federal Trade Commission's (FTC) cybersecurity advice Web site remained offline January 25, a day after it had been hacked by the group Anonymous in a continuing protest over proposed anti-piracy laws and recent anti-piracy arrests. The OnGuardOnline.gov site, intended to give people cybersecurity advice, was hacked January 24, with the home page replaced by the Anonymous logo, a rap song, and a message threatening more attacks if anti-piracy legislation in Congress, which has stalled after a massive online protest January 18, were to pass. The FTC, which operates the site with several other agencies, took it offline after the hack. Source: http://gcn.com/articles/2012/01/25/ftc-anonymous-hack-sopa-megaupload-fallout.aspx

New data leak: VA releases info on 2,200 vets. The Department of Veterans Affairs said January 20 that personal information for more than 2,200 veterans was posted on Ancestry.com after it mistakenly released the data through the Freedom of Information Act (FOIA). There is no indication the information was misused, but the agency is still notifying all potentially affected veterans and is offering free credit monitoring. Ancestry.com removed the data as soon as the VA alerted it to the department's mistake. While the VA was required to release the requested records under the FOIA, somehow information about living veterans was released as part of a database about deceased veterans. The department said it is investigating how the mistake happened. Source: http://www.militarytimes.com/news/2012/01/ap-veterans-affairs-va-releases-info-2200-veterans-012012/

(Illinois; Pennsylvania) **Police: Joliet man threatened to kill Social Security staff.** A Joliet, Illinois man upset with reductions to his benefits allegedly threatened to kill employees at a Social Security Administration (SSA) office in Wilkes Barre, Pennsylvania, the week of January 16, the

Joliet Herald-News reported January 22. The DHS took the man's reported threats seriously enough to have local police obtain a warrant for his arrest, an official said. SSA employees notified the DHS and because of the man's criminal history, federal agents asked Joliet police to pursue the case. A detective obtained an arrest warrant January 20 against the man with a $100,000 bond. He was being sought for harassment by telephone, a Class 4 felony that can carry a 1- to 3-year prison sentence and a $25,000 fine. Source: http://heraldnews.suntimes.com/news/10139661-418/police-joliet-man-threatened-to-kill-social-security-staff.html

(Washington) **Phishers bait city workers in Seattle with phony speeding tickets.** Hundreds of government employees in Seattle received fraudulent e-mails January 19 that appeared to be traffic violation notifications, but were, in fact, vehicles for infection by malicious software. According to the Microsoft Malware Protection Center and the Seattle Police Department, hundreds of individuals with Seattle.gov e-mail addresses began receiving the fraudulent parking ticket announcements January 19. The messages have the subject "Seattle Traffic Ticket" and claim the recipient committed one of a number of violations, including speeding. Clicking a hyperlink in the e-mail message loaded an iframe that redirects users to a Ukrainian IP address. According to TechNet, the site contains an obfuscated JavaScript that exploits a bug in the Microsoft Data Access Components (MDAC) that was patched in 2006. If successful, the exploit will download an executable from a .ru domain. Windows is detecting the file as Worm:Won32/Cridex.B. The malware attempts to connect via SSL to "jahramainso[dot]com." The malware can also update itself by communicating with its command and control server. The host appears to be deploying the same file at present that was detected in the initial infection, but the authors may try to evade detection by altering the host with which it communicates. Source: http://threatpost.com/en_us/blogs/phishers-bait-city-workers-seattle-phony-speeding-tickets-012012

Information Technology and Telecommunications

Facebook scammers leverage the Amazon Cloud. Recently, spammers began using Amazon's cloud services for hosting fake Facebook pages leading to surveys because it is cheap and because is less likely Facebook will block links from an Amazon domain. Users are usually reeled in with offers to see a funny/amazing/shocking video, and click on the offered URL (often a shortened one). In a recently spotted scam, users who click the link are taken to a fake Facebook page where those who use Chrome and Firefox are asked to install a fake YouTube plug-in to view the video. The offered plugin is not what it claims to be. "Upon installing the plugin, a redirector URL is generated by randomly selecting from the usernames, mo1tor to mo15tor, in the Amazon web service," explain F-Secure researchers. "Then, the link generated is shortened through bitly.com via the use of any of the 5 hardcoded userID and API key-pairs. These key-pars gives a spammer the ability to auto-generate bit.ly URLs for the Amazon web service link. This ultimately leads to a redirection to the fake Facebook page." These users are, therefore, responsible for propagating the scam further by unknowingly posting the scam message on their Facebook profiles, and are not asked to fill out surveys. Users who use other browsers are spared from inadvertently spamming their friends but are redirected to surveys provided by affiliate marketers. Source: http://www.net-security.org/secworld.php?id=12301

Symantec advises users to turn off pcAnywhere in hack aftermath. Symantec has advised customers to take their copies of pcAnywhere offline as the company continues to struggle with the aftermath of a major data breach. The company issued a whitepaper addressing new vulnerabilities in its remote access tool that were exploited by a recently publicized attack which allowed attackers to gain access to the application's source code. The 2006 hack was recently brought to light by an Indian hacking team that is seeking to publicly distribute the code. Symantec has now determined a major update is necessary to protect users from any flaws revealed in the compromised source code. The company is advising users of pcAnywhere 12.5 to disable the remote management tool until an update is released. If users do not take their copies of the tool offline, the company warned attackers could possibly compromise systems and perform "man-in-the-middle" attacks that could result in the theft of user credentials and other network traffic. Source: http://www.v3.co.uk/v3-uk/news/2141452/symantec-advises-users-pcanywhere-hack-aftermath

Super-powered 'frankenmalware' strains detected in the wild. Viruses are accidentally infecting worms on victims' computers, creating super-powered strains of hybrid software nasties. The monster malware spreads quicker than before, screws up systems worse than ever, and exposes private data in a way not even envisioned by the original virus writers. A study by antivirus outfit BitDefender found 40,000 such "Frankenmalware samples" in a study of 10 million infected files in early January, or 0.4 percent of malware strains sampled. These cybercrime chimeras pose a greater risk to infected users than standard malware, the antivirus firm warns. "If you get one of these hybrids on your system, you could be facing financial troubles, computer problems, identity theft, and a wave of spam thrown in as a random bonus," said the BitDefender analyst who carried out the study. "The advent of malware sandwiches throws a new twist into the world of malware. They spread more efficiently, and will become increasingly difficult to predict." BitDefender does not have historical data to go on. Even so, it posits that frankenmalware is likely to grow at the same rate as regular computer viruses, or about 17 percent per year. All of the malware hybrids analyzed by BitDefender so far have been created accidentally. However, the risk posed by these combinations could increase dramatically as criminals latch onto the idea. Source: http://www.theregister.co.uk/2012/01/25/frankenmalware/

Researchers discover network of 7,000 typo squatting domains. A network of some 7,000 typo squatting domains is being used by scammers to effectively drive traffic towards their sites, some of which get so much traffic that they managed to enter Alexa's top 250 list of sites with the largest Web traffic, according to Websense researchers. The typo squatting domains take advantage of visitors to popular Web sites such as Google, Twitter, Gmail, YouTube, Wikipedia, Victoria's Secret, Craigslist, and many more, and redirect them to spam survey sites. From there, the users are taken to sites with spam advertisements and greyware masquerading as free downloads of legitimate software such as movie downloaders. Websense researchers said currently these sites are not offering malware for download. "However, if these networks are resold to underground groups, then the potential outcome could be even more damaging than the 0-day exploit security attacks," they point out. Users are mostly in danger of handing over their private information and other sensitive data when completing the surveys. Source: http://www.net-security.org/secworld.php?id=12275

10K reasons to worry about critical infrastructure. A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public Internet, including water and sewage plants, and found many could be open to easy hack attacks, due to lax security practices. Infrastructure software vendors and critical infrastructure owners have long maintained industrial control systems — even if rife with security vulnerabilities — are not at risk of penetration by outsiders because they are not online. However, a computer science doctoral student from Cambridge University developed a tool that matches information about industrial control systems connected to the Internet with information about known vulnerabilities to show how easy it could be for an attacker to locate and target them. To debunk the myth industrial control systems are never connected to the Internet, the student used the SHODAN search engine, which allows users to find Internet-connected devices using simple search terms. He then matched that data to information from vulnerability databases to find known security holes and exploits that could be used to hijack the systems or crash them. He used Timemap to chart the information on Google maps, along with red markers noting brand devices that are known to have security holes in them. The student found 10,358 devices connected through a search of 2 years worth of data in the SHODAN database. However, he was unable to determine how many of the devices uncovered were actually working systems, nor was he able to determine in all cases whether the systems were critical infrastructure systems installed at power plants and other significant facilities. The student also found only 17 percent of the systems he found online asked him for authorization to connect, suggesting administrators either were not aware their systems were online or had simply failed to install secure gateways to keep out intruders. Source: http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

Black hat cleaning day: Phantom leaks tons of data. Notorious black hats that hacked thousands of Web sites in their lifetime gather gigabytes of information stolen from their victims, much of which is never published online. Phantom, one of the members of TeaMp0isoN, decided to clean up his hard drive and publish data he collected as a result of breaching sites, Softpedia reported January 23. Usernames, passwords, and other sensitive information belonging to members and administrators of around 7,000 Web sites are contained in the data leak, posted on Pastebin in multiple parts. The list of victims includes book stores, Web site developers, mobile phone stores, and other, mostly commercial, Web sites from all around the world. Source: http://news.softpedia.com/news/Black-Hat-Cleaning-Day-Phantom-Leaks-Tons-of-Data-Exclusive-248076.shtml

Anonymous dupes users into joining Megaupload attack. In a message on Twitter and in a blog post, Anonymous claimed its January 20 distributed denial of service (DDoS) attacks against the Web sites of the Department of Justice, the Recording Industry Association of America, the Motion Picture Association of America, and others were its largest ever, and 5,600 people collaborated in the assaults. However, some of the 5,600 who participated may have done so unwittingly, said a senior technology consultant with Sophos. He said members of Anonymous distributed links via Twitter and elsewhere that when clicked, automatically launched a Web version of Anonymous's DDoS tool, the Low Orbit Ion Cannon (LOIC). The links pointed to a page on PasteHTML.com, a free HTML code-hosting site, which in turn executed some JavaScript to fire LOIC at Anonymous-designated targets. Many of those messages said nothing about LOIC or that clicking the link tricked the user into the DDoS attack, the consultant said. Anonymous is still recruiting people to its campaign. A search of Twitter using a string published on Gawker.com indicated the link was being shared January 20 at the rate of about 10 to 18 times per minute. Source: http://www.computerworld.com/s/article/9223601/Anonymous_dupes_users_into_joining_Megaupload_attack?taxonomyId=17

Hackers prove EA, IGN, ImageShack, NY Times, Verizon vulnerable. A new hacking collective, TeamHav0k, launched an operation called "#OP XSS" in which they try to find cross-site scripting (XSS) vulnerabilities in major Web sites. The first results of the operation came in and reveals many important sites contain XSS flaws. A Pastebin document reveals Web sites such as the ones belonging to Verizon, Huffington Post, European Organization for Nuclear Research, Electronic Arts (EA), IGN, and New York Times contain design flaws. Some educational institutions were also found to contain XSS security holes, including University of Illinois, Harvard, Yale, and Rockefeller University. Telecoms company Verizon, media hosting company ImageShack, value calculator and traffic estimator tool StatShow, Major League Gaming, and Dr. Pepper complete the list. Even though XSS vulnerabilities are among the most common ones found in commercial Web sites, this does not mean they are not dangerous. Cybercriminals can rely on these weaknesses to execute their own malicious codes and cause damage to the virtual assets of unsuspecting Internet users. Source: http://news.softpedia.com/news/Hackers-Prove-EA-IGN-ImageShack-NY-Times-Verizon-Vulnerable-247952.shtml

National Monuments and Icons

(Virginia) **Arlington Cemetery trying to account for missing $12 million.** Arlington National Cemetery is trying to account for $12 million — about a quarter of its current annual budget — that was allocated to the cemetery between 2004 and 2010 but apparently was never spent. Congressional leaders and federal investigators who have been probing the cemetery's operations said at a Senate hearing January 25 there was no documentation detailing where the funds are or how such a large amount of taxpayer money could have gone missing. A Senator called the hearing as part of continued oversight of the cemetery, the nation's premier military burial ground, which has spent the past 18 months attempting to fix problems with burial procedures, contracting, and management. In 2010, Army investigators found people had been buried in the wrong places, unmarked or mismarked grave sites, and that millions had been spent on contracts that produced nothing. The Army's Criminal Investigation Command and the FBI are conducting an investigation into possible contracting fraud and falsification of records. The Army's inspector general testified his office would continue to monitor the cemetery's finances annually. He said the missing money was troubling because the cemetery's previous management had asserted "they were short of funds when in fact they had funds they couldn't account for." The director of the Army National Cemeteries Program said the cemetery's accounting procedures were pdated since she took over in 2010 so that every dollar allocated to the cemetery is accounted for. The cemetery's annual budget is $45 million, a spokeswoman said. The missing $12 million was part of $27 million in unspent funds found by the auditors. So far, $15 million of that has been recovered, cemetery officials said, although it is not clear how the money was found. Source: http://www.washingtonpost.com/local/arlington-national-cemetery-trying-to-account-for-missing-12million/2012/01/25/gIQActihRQ_story.html

NARA faulted for internet connection outage that affected staff and public. An Internet connection blackout at the National Archives and Records Administration (NARA) cut off all staff access to the Web, and all public access to agency Web sites for 32 hours, according to a newly disclosed report from the archives' Inspector General (IG). The outage occurred in September, but was only recently disclosed publicly. The failed Internet connection due to a cut fiber-optic cable "significantly affected" NARA operations and hampered "critical" staff work, the IG wrote in a management letter about the incident published on his office's Web site. The outage also apparently hampered members of the public who unexpectedly lost access to the NARA site. The incident indicated the NARA does not have a backup connection to restore Internet and other services within a timely manner, the IG wrote. He said he would audit the connections and continuity of operations functions in coming weeks. "NARA officials overseeing the network architecture should have known the design of the network created a single point of failure, and taken action to address this risk before NARA's mission and business capabilities were impacted," the IG wrote. The letter was dated October 13, but only recently was published on the agency's Web site. Source: http://fcw.com/articles/2012/01/24/nara-faulted-for-internet-outage-that-affected-staff-and-public.aspx

(California) **Man crushed by tree at Yosemite as storm batters California.** A part-time ranger at Yosemite National Park was killed January 22 when strong winds felled a tree and crushed him in his tent in an employee housing area of the park, officials said. The man had worked in the park for 5 years and was employed by a ski area concessionaire, according to a park spokesman. A large tree limb crushed the employee's tent in Yosemite Valley, and strong winds knocked down trees around the park. The storm lingered in the state throughout the day, causing flooding in the north and power outages in Palm Springs, Joshua Tree, and Cathedral City. Source: http://latimesblogs.latimes.com/lanow/2012/01/man-crushed-by-tree-at-yosemite-as-winter-storm-batters-state.html

Postal and Shipping

(Utah) **FedEx employee charged with terrorism threat for making bomb joke at Utah Army base.** Prosecutors in Utah charged a FedEx driver with a threat of terrorism count over allegations he joked that a package he was delivering to a Utah Army base was likely a bomb. Charges filed January 25 in Salt Lake City show the deliveryman was dropping off a package

September 20 addressed to a U.S Army Corps of Engineers employee at Camp Williams in Salt Lake City. Prosecutors said when a woman asked him what it was, he replied that it was probably a bomb. Military police then evacuated 215 people from the building and the surrounding area. He is charged with a third-degree felony count of threat of terrorism. Source: http://www.washingtonpost.com/national/fedex-employee-charged-with-terrorism-threat-for-making-bomb-joke-at-utah-army-base/2012/01/26/gIQAH7vzSQ_story.html

National strategy for global supply chain security announced. Pandemics, natural disasters, or attacks involving weapons of mass destruction could undermine the continuity of the global supply chain system as a whole. Because of the interconnectedness of the system, even smaller, localized events could escalate rapidly and cause significant disruptions. The White House announced January 25 the National Strategy for Global Supply Chain Security, an important step to strengthen and protect the global supply chain system. The strategy, focused on the worldwide network of transportation, postal, and shipping assets and supporting infrastructures, articulates the nation's vision and approach, and encourages collaborative implementation with key state, local, tribal, territorial, private sector, and international stakeholders. Source: http://www.whitehouse.gov/blog/2012/01/25/national-strategy-global-supply-chain-security-announced

Public Health

Chemicals used during medical imaging tests may damage thyroid. Chemicals used to enhance pictures obtained from medical imaging tests may lead to overactive or underactive thyroid glands, a study released January 23 by in the Archives of Internal Medicine showed. Patients injected with contrast material were about twice as likely as those who did not get the chemical to develop hyperthyroidism, when the gland produces too much thyroid hormone and can cause rapid or irregular heart rates. Results also showed an increased risk for hypothyroidism. The use of the chemicals, called iodinated contrast media, has risen in the past two decades as more people get computed tomography scans and heart catheterizations, which are used to diagnose and treat some heart conditions, the researchers said. They looked at patients from January 1990 to June 2010 who did not have any thyroid disease. They also checked to see if they were exposed to iodinated contrast media. They found 178 people developed hyperthyroidism, and, of those, 11 percent received contrast agents. The study also showed 213 developed hypothyroidism and of those, 12 percent received contrast agents. Those who used contrast were 1.5 times more likely than those who did not to develop hypothyroidism, a finding the researchers could not rule out was due to chance. Source: http://news.businessweek.com/article.asp?documentKey=1376-LY9KLW6JTSEC01-0IFO4CO79V1L7EUJAU5BJT6SMD

Anti-infective drug shortages pose threat to public health and patient care. A review published in Clinical Infectious Diseases stated that shortages of key drugs used to fight infections represent a public health emergency and can put patients at risk, the Infectious Diseases Society of America stated in a January 20 news release. Frequent anti-infective shortages can substantially alter clinical care and may lead to worse outcomes for patients, particularly as the development of new anti-infectives has slowed and the prevalence of multidrug-resistant pathogens is increasing. First-line treatments for herpes encephalitis, neurosyphilis, tuberculosis, and enterococcal infections, among others, have been hit by shortages, forcing physicians to use other drugs that may not work as well, the authors found. Of the 193 medications unavailable in the United States at the time of the analysis, 13 percent were anti-infective drugs, the authors found. “Anti-infectives often represent irreplaceable life-saving treatments,” the authors noted, and hospitalized patients are particularly vulnerable in an era when such shortages often last months and are occurring more frequently. Source: http://esciencenews.com/articles/2012/01/22/anti.infective.drug.shortages.pose.threat.public.health.and.patient.care

Transportation

(Indiana) **Train traffic to be suspended for Super Bowl.** Train tracks that run within a block of Lucas Oil Stadium in Indianapolis, Indiana, will be empty come Super Bowl Sunday (February 5). As part of the overall public safety plan to reduce the possibility of a hazardous chemical incident or a terrorist threat near the National Football League’s championship game, CSX agreed to suspend operations 3 hours before the game until 2 hours afterward. “(CSX is) going to monitor the rail line for us, east and west of downtown,” said the head of the Indianapolis division of Homeland Security. “On game day, we won’t allow any rail traffic through prior to the game and after the game.” The railroad will also conduct a rigorous inspection of rail cars at rail yards in Anderson and Avon. “They’ll have inspections of freight coming through the week prior to the game just to ensure that there’s no hazardous material that is coming through that could be a threat,” he said. Source: http://www.theindychannel.com/news/30281153/detail.html

Hackers manipulated railway computers, TSA memo says. Hackers, possibly from abroad, executed an attack on a Northwest rail company’s computers that disrupted railway signals for 2 days in December, according to a government memo recapping outreach with the transportation sector during the emergency. On December 1, train service on the unnamed railroad “was slowed for a short while” and rail schedules were delayed about 15 minutes after the interference, stated a Transportation Security Administration (TSA) summary of a December 20 meeting about the episode obtained by Nextgov. The following day, shortly before rush hour, a “second event occurred” that did not affect schedules, TSA officials added. On January 23, officials at the DHS said that following additional in-depth analysis, it appears the rail infiltration may not have been a targeted attack. “On December 1, a Pacific Northwest transportation entity reported that a potential cyber incident could affect train service,” a DHS spokesman said. “The Department of Homeland Security, the FBI, and our federal partners remained in communication with representatives from the transportation entity in support of their mitigation activities and with state and local government officials to send alerts to notify the transportation community of the anomalous activity as it was occurring.” Source: http://www.nextgov.com/nextgov/ng_20120123_3491.php

Water and Dams

Damage from 2011 floods could mean worse in 2012. Damage from last year's record spring floods could leave many people along the Mississippi River in even more danger this year, the U.S. Army Corps of Engineers said January 26. It says it is assessing the damage to levees, structures and navigation channels, and will begin notifying affected communities of problem areas in February. The regional flood risk manager for the Mississippi Valley Division said the Corps will use a Web-based application called CorpsMap and information papers to send out the data. The Corps said in December there was a significant risk of more flooding along the Birds Point Floodway, where it blew three holes in a levee to relieve pressure as floods threatened nearby Cairo, Illinois. "A couple more areas that we haven't fixed but know where they are, are where the river tried to change course," a Corps spokesman said. The biggest of those was just north of Tiptonville, Tennessee. Another, less seriously damaged area is north of Louisiana's Old River Control Structure. Most of the damage along the Mississippi River is from St. Louis south, he said. Source: http://www.stltoday.com/news/state-and-regional/missouri/damage-from-floods-could-mean-worse-in/article_1268ded3-707a-571f-ae10-212d92af1a8d.html

(Oregon) **Rivers on the rise once again.** A new round of rainstorms has some Eugene, Oregon residents on edge as streams push close to overtopping their banks because dams upstream are boosting outflows to make room for more rain. Long Tom River, which swelled after Fern Ridge Lake filled to 75 percent of its capacity following a week of rainy weather, prompted the U.S. Army Corps of Engineers to release 4,000 cubic feet of water per second (cfs) from the dam to rebuild the lake's storage capacity to handle the rain the week of January 23. Officials at the Corps' Portland office said the large releases are needed to prevent worse flooding from storms yet to come. Some reservoirs had to be lowered quickly or they had the potential to overfill with more rainfall, forcing larger releases and more dangerous flooding. Waters in the southern Willamette Valley could come within less than a foot of flood stage January 25. Other rivers, including the Long Tom near Monroe and the Willamette River at Harrisburg, were above bank full January 24, and the latter could come within less than a foot of flood stage later. Similar crests are expected later in Corvallis, Albany, and Salem. Eugene received more than 1.7 inches of rain January 24, more than initially forecast and a record for the date. That prompted hydrologists to raise the expected crests on local rivers as the additional water runs off and moves downstream. More rain is forecast until January 26 from the current string of storms. The extra rain has renewed fear of landslides, which occurred throughout Western Oregon the week of January 16, including one that closed Highway 126 between Vida and Blue River for most of a day. Source: http://www.registerguard.com/web/updates/27510909-55/river-flood-tom-corps-forecast.html.csp

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND

ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168